# Extreme DDoS Defense (XD3)

Stuart Wagner
Program Manager
Information Innovation Office (I2O)
DARPA

September 2, 2015

# Agenda


| TIME | EVENT | SPEAKER |
|---|---|---|
| 1330 - 1430 | **Registration** | |
| 1430 - 1440 | **DARPA Security** | Marissa Sylvester – DARPA SID |
| 1440 - 1445 | **Welcoming Comments** | Stu Wagner – DARPA I2O |
| 1445 - 1500 | **DARPA CMO** | Mark Jones – DARPA CMO |
| 1500 - 1520 | **XD3 Program Discussion** | Stu Wagner – DARPA I2O |
| 1520 - 1600 | **Break** | |
| 1600 - 1630 | **Program Q&A** | |

# Extreme DDoS Defense (XD3)

Mark Jones
Contracting Officer
Contracts Management Office (CMO)
DARPA

September 2, 2015

## DISCLAIMER

The published BAA is the official solicitation instructions that must be followed in order to submit a responsive proposal. If anything said or addressed during this presentation or in the FAQ conflicts with the published solicitation, the BAA takes precedence.

The Government may issue amendments to the BAA to effect any changes deemed necessary in response to the FAQ. Such amendments would be posted to FBO and Grants.gov prior to the solicitation closing date and would supersede previous versions of the solicitation.

## BAA OVERVIEW

BAA follows procedures in accordance with FAR 35.016.

BAA is posted on FEDBIZOPPS at www.fbo.gov and Grants.gov at http://www.grants.gov/ (as well as amendments).

BAA allows for a variety of technical solutions.

Proposals due by 12:00 noon ET on October 13, 2015.

BAA covers all info needed to submit proposals. Follow instructions for proposal preparation and submittal.

The BAA FAQ and slides from this meeting will be posted to http://www.darpa.mil/work-with-us/opportunities/darpa-baa-15-56.

## POTENTIAL AWARD INFORMATION

- Five Technical Areas (TAs); anticipate multiple awards in TAs 1-3, and TA5. TA4 may be options under TA 1-3 awards.
- May submit proposals against any and all TAs, but shall not submit proposals combining TAs (with TA4 an exception). All TA 1-3 proposers must propose optional TA4. No TA4 only proposals.
- Conflicts of interest between TA1-3 vs TA5 – If single entity submits proposals against multiple TAs, this may create a conflict that would be resolved at the Government's discretion.
- Awards may be Procurement Contracts, Cooperative Agreements or Other Transaction Agreements (OTs). No grants will be awarded.
- Program Stresses Open Exchange of Information – will utilize Associate Contractor Agreement contract clause (or similar condition in non contract awards).
- Award amounts have not been predetermined and will depend on the quality of the proposals received and the availability of funds.

# ELIGIBILITY

All interested/qualified sources may respond subject to the parameters outlined in the BAA.

Foreign organization/individuals – check all applicable Security Regulations, Export Control Laws, Non-Disclosure Agreements, and other applicable governing statutes.

FFRDCs and Government entities

- Subject to applicable direct competition limitations
- Must clearly demonstrate eligibility per BAA

Real and/or Perceived Conflicts of Interest

- Identify any conflict
- Include mitigation plan

Ability to support classified activities – TA5 - TS / TAs 1-3 – Secret (as required)

# PROPOSAL PREPARATION INFORMATION

- Proposals consist of two volumes – Technical and Cost
- Volume 1 - Technical and Management
  - Volume 1 has maximum 32 page limit
  - Includes mandatory Appendix A (does not count towards page limit)
  - Includes optional Appendix B (does not count towards page limit)
- Volume 2 – Cost (No page limit)
- The BAA will describe the necessary information to address in each volume
    - Make sure to include every section identified
    - If a section does not apply – put “None” (e.g., Animal Use – None, OCI - None)
    - Include a working/unprotected spreadsheet as part of your Cost Volume submission
    - Review individual TA descriptions, IP and the deliverables section for submittal information
    - Volume 1 – strive for brevity and clarity

## PROPOSAL PREPARATION TIPS

- **Statement of Work (SOW)** – Write a SOW as if it were an attachment to a contract
  - Don't use proposal language (e.g. we propose to do . . .)
  - Break out work between any phases/time periods identified in the BAA
  - Succinctly and clearly define tasks & subtasks
  - Do not include any proprietary information!

- **Risk** – Do not be afraid to address Risk in Technical Volume
  - Identify risk(s) to show an understanding of technical challenge(s)
  - Discuss potential mitigation plans / alternative directions

## PROPOSAL PREP – INTELLECTUAL PROPERTY RIGHTS

Government desires, at a minimum, **Government Purpose Rights** for any proposed noncommercial software and technical data. (SEE DFARS 227 for Patent, Data, and Copyrights)

Since XD3 will emphasize creating and leveraging open architecture technology, IP rights and software licenses asserted by proposers are strongly encouraged to be aligned with this goal.

Data Rights Assertions – IF asserting **less than Unlimited Rights**:

- Provide and justify basis of assertions
- Explain how the Government will be able to reach its program goals (including transition) within the proprietary model offered; and
- Provide possible nonproprietary alternatives

IF proposed solution utilizes commercial IP – submit copies of license with proposal

## ITEMS TO NOTE

Work expected to be fundamental research – don't anticipate publication restrictions unless proposed effort is determined non fundamental.

Indicate in proposal whether or not the scope is believed to be fundamental on both prime and subcontractor effort.

Understand and comply with SAM, E-verify, FAPIIS, i-Edison and WAWF. Links are found in the BAA.

Subcontracting Issues:

- Non-Small Businesses - Subcontracting Plans required for FAR-based contracts expected to exceed $650,000 (**effective Oct 1 – limit will rise to $700,000**).
- Subcontractor/subawardee cost - Proposals must include, at a minimum, a non-proprietary, subcontractor proposal for EACH subcontractor.
- If utilizing FFRDC, Government entity, or a foreign-owned firm as a subcontractor, submit their required eligibility information, as applicable.

## ITEMS TO NOTE CONTINUED

Proposals must be valid for a minimum of 120 days – Recommend at least 150 days to accommodate holiday delays

If a prospective proposer believes a conflict of interest exists or has a question on what constitutes a conflict - promptly raise the issue with DARPA

New threshold limits as of Oct 1, 2015 – DARPA to issue BAA amendment

Document files must be in .pdf, .odx, .doc, .docx, .xls, and/or .xlsx formats.

Submissions must be written in English.

## PROPOSAL SUBMISSION

- Submissions will be UNCLASSIFIED - classified submissions will NOT be accepted.
- DO NOT submit proposals except as outlined in the BAA (e.g., email/fax submissions will NOT be accepted).
- Use only one method for submitting a proposal.
- Proposals for Cooperative Agreements will utilize the Grants.gov website for uploading proposals.
- Proposals for Procurement Contracts/OTAs will utilize DARPA's web-based upload system:
  - If not previously registered – 2 step registration process
  - Submission must be in a single zip file not exceeding 50 MB
  - When submitting – make sure to drop files in correct BAA
  - Must **FINALIZE** submission prior to closing to be considered

**DO NOT WAIT UNTIL THE LAST DAY TO BEGIN REGISTRATION / PROPOSAL SUBMISSION PROCESS**

## EVALUATION / AWARD

No common Statement of Work - Proposal evaluated on individual merit and relevance as it relates to the stated research goals/objectives

Evaluation Criteria (listed in descending order of importance) are: (a) Overall Scientific and Technical Merit; (b) Potential Contribution and Relevance to the DARPA Mission; and (c) Cost Realism.

Evaluation done by scientific/technical review process. DARPA SETAs with NDAs may assist in process.

Government reserves the right to select for award all, some, or none of the proposals received, to award portions of a proposal, and to award with or without discussions.

## COMMUNICATION

Prior to Receipt of Proposals – No restrictions, however Gov't (PM/PCO) shall not dictate solutions or transfer technology. Unclassified FAQs will be periodically posted to this BAA's DARPA web page.

After Receipt of Proposals – Prior to Selection: Limited to PCO – typical communication to address proposal clarifications.

After Selection/Prior to Award: Communications range from technical clarifications/revisions to formal cost negotiations. May involve technical as well as contracting staff.

Informal feedback for proposals not selected for funding may be provided once the selection(s), if any, are made.

**Only a duly authorized Contracting/Grants Officer may obligate the Government**

## TAKE AWAY

Submit proposals before the due date/time - Do NOT wait until the last minute to submit.

Read and understand the BAA - Follow the BAA when preparing proposals.

Be familiar with Government IP terms from the DFARS Part 227.

Submit working/unprotected spreadsheet(s).

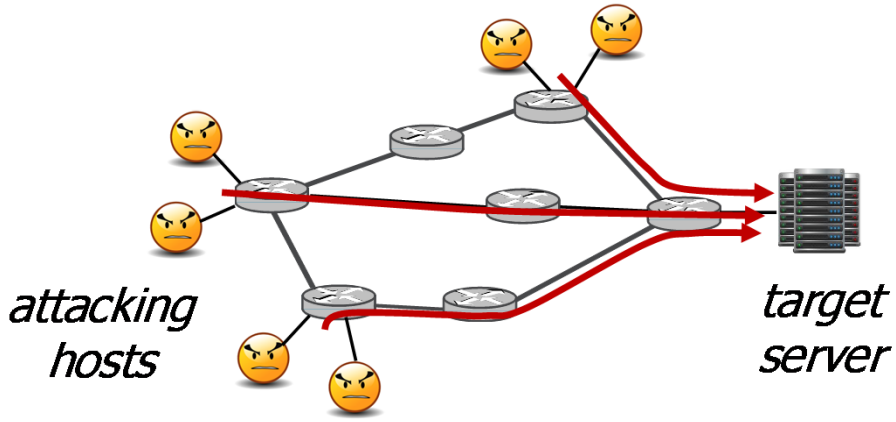
The Contracting/Grants Officer is the only Government official authorized to obligate the Government.

# Extreme DDoS Defense (XD3)

Stuart Wagner
Program Manager
Information Innovation Office (I2O)
DARPA

September 2, 2015

# DDoS Attacks: A Major Threat to Mission Success




- Adversary-controlled, networked hosts acting in concert to overwhelm a target machine or network link by sending traffic that:
  - Exhausts the transmission capacity of the target, or
  - Exhausts the CPU or memory of the target
- DDoS attacks are responsible for ~1/3 of downtime events worldwide
- Examples DDoS mechanisms in use today:
  - Botnets (black-market rentals available for $150/week)
  - Man-in-the-Middle attacks that achieve effects similar to botnets
  - Low-volume, precision attacks that achieve vastly disproportionate damage


# Current Art and Its Limitations

- Defensive responses are reactive, manually driven and too slow
- Low-volume attacks exceedingly difficult to diagnose and defeat with in-line intrusion detection and “scrubbing”
- In-line inspection of flows not useful for encrypted traffic and pose scalability problems
- Defenses must protect real-time, transactional services as well as cloud computing capabilities, not just static content storage
- It is too easy for attackers to characterize their targets and to plan their attacks

XD3 goal: a vast improvement in inherent resilience against DDoS attacks through both proactive and reactive means

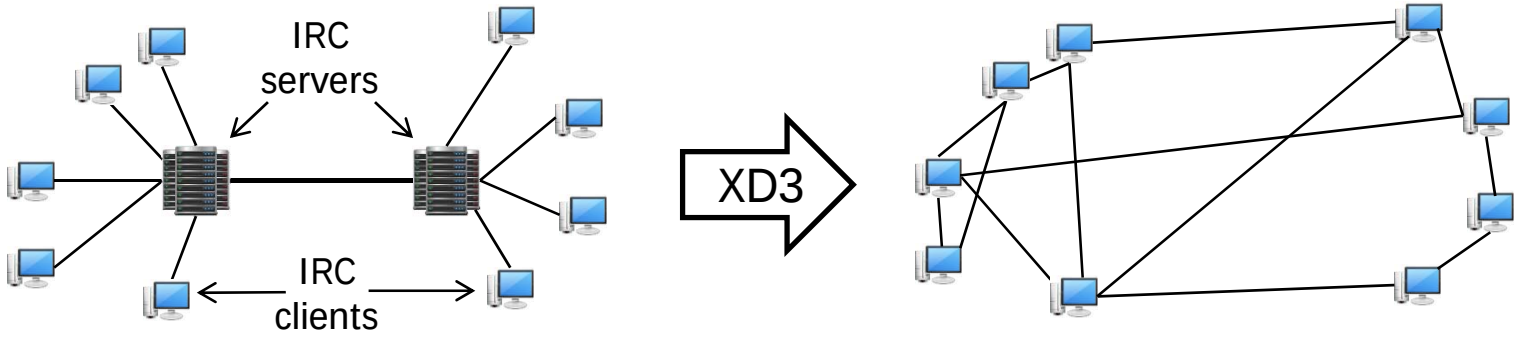
# XD3 Concepts for DDoS Resilience

| Weakness of Current Art | XD3 Concept | Rationale and Impact |
|---|---|---|
| Concentrated locus of information and computing makes it easy to locate targets (data centers, servers) | Manageable Dispersion of Cyber Resources (Technical Area 1) | Spreads physical or logical locations of cyber resources to mitigate centralized points of vulnerability |
| Static, predictable behavior of targets facilitates attack planning and execution | Networked Maneuver (Technical Area 2) | Greatly increases attacker work factor in planning and executing focused DDoS; can deflect DDoS in ways that minimize damage |
| Low-volume DDoS can hide in "noise" of ambient traffic, defeating in-line intrusion detection systems | Adaptive Endpoint Sensing and Response (Technical Area 3) | Enables reliable detection, and point-of-attack mitigation, for low-volume DDoS attacks that find their targets |

*Disperse* the cyber assets, *Disguise* those assets, and *Mitigate* the attacks that still make it through

# Manageable Dispersion of Cyber Resources (TA1)

XD3 vision: distribute the locus of cyber capabilities (cloud computing, C2,...), while retaining the performance of today's centralized server architectures



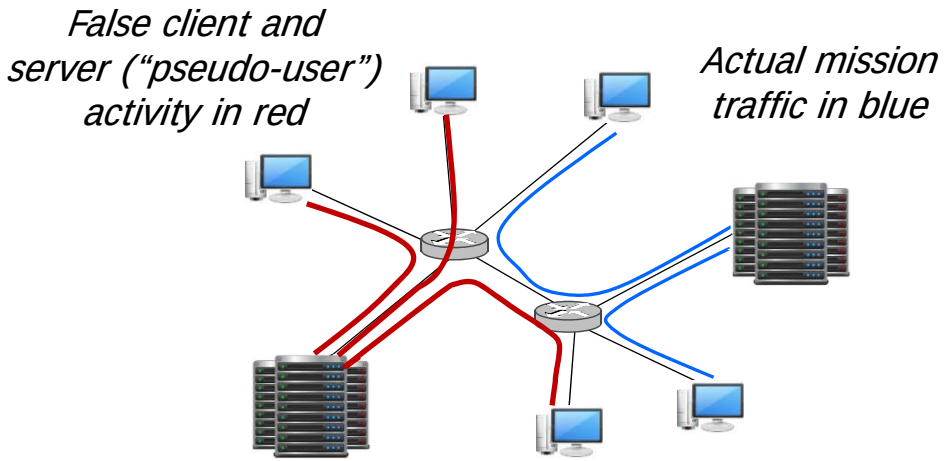

*"Each IRC server acts as a central server for the network it sees" – IETF RFC 2810*

*Distributed, and possibly peer-to-peer (P2P), messaging and storage*

- Internet Relay Chat (IRC) remains a critical protocol and architecture for DoD command and control, but it has known vulnerabilities
- Can we devise more-resilient, dispersed architectures and protocols for computing and C2 (as the botnet builders have done with P2P)?
- Challenges: accounting for realistic network conditions, including attacks; maintaining high performance in absence of attacks

# Networked Maneuver for DDoS Defense (TA2)

- Develop *network-oriented* (as opposed to single-host) techniques
- Devise means of *deception* as well as *obfuscation*




Obfuscation: create uniform activity patterns in network and/or servers, to make mission difficult to characterize

Deception: Present adversary with a structured "false reality", with bulk of activity at different locations or times w/r to actual mission

TA2 Challenges:

- Minimize and validate level of interference with legitimate users
- Enable informed adjustment of maneuver in response to attack
- Provide commanders with means of assessing effectiveness of maneuver, both before and during operation

# Adaptive Endpoint Sensing and Response (TA3)

The response to low-volume DDoS **must** incorporate knowledge of the attacked host's state and **must** be able to adapt the host's operation

Potential XD3 Approach:

- Instrumentation of host kernel and application programs
- Correlation of state (CPU, memory, queues,…) with I/O activity
- Adapt host operation (state machines, protocol logic) on the fly to mitigate the attack
  - Current state machines assume that all communicating participants adhere to the rules of the protocol
  - These state machines were not designed to deal with bad behavior

| Challenge | Metrics |
|---|---|
| "Do no harm" when adapting state machines and protocols | No more than 1% degradation of throughput in absence of attack |
| Converge rapidly to most effective attack response | Response time < 60 sec (Phase 1) and < 10 sec (Phase 2); >90% recovery of application utility |

# XD3 Program Structure

| Program Technical Area | | Role and Outputs |
|---|---|---|
| 1 | Manageable Dispersion of Cyber Resources | • In Phase 1, teams design algorithms and prototype systems in their respective technical areas, and conduct experiments<br>• Phase 2 continues this experimentation while pursuing opportunities for cross-performer integration |
| 2 | Networked Maneuver | |
| 3 | Adaptive Endpoint Sensing and Response | |
| 4 | Technology Integration (Phase 2) | • Synergistic performers from TAs 1-3 integrate their components |
| 5 | Voice of the Offense | • Recommends DDoS attack scenarios for testing within TAs 1-4<br>• Periodically reviews designs of TAs 1-4 to identify weaknesses and vulnerabilities proactively |

# XD3 Notional Program Schedule and Milestones

| Program Phase | Phase 1 | | | | | | | | | | | | | | | | | Phase 2 | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Fiscal Year | 16 | | | | | | 17 | | | | | | | | | | | 18 | | | | | | | | | | | 19 | | | | | |
| Program Month | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 |
| Kickoff and PI Meetings | ◆ | | | | | ◆ | | | | | | ◆ | | | | | | ◆ | | | | | | ◆ | | | | | | ◆ | | | | | | |
| Proposed Test Plans | | | ◆ | | | | | ◆ | | | | | | ◆ | | | | | | ◆ | | | | | ◆ | | | | | ◆ | | | | ◆ | | |
| TA Component Expts | | | | ◆ | | | | | ◆ | | | | | | ◆ | | | | | | | | | | | | | | | | | | | | | |
| System Expts | | | | | | | | | ◆ | | | | | | ◆ | | | | | | ◆ | | | | | | ◆ | | | | | ◆ | | | | ◆ |
| Integration Plan | | | | | | | | | | | | | | | | ◆ | | | | | | ◆ | | | | | | | | | | | | | | |
| Voice of Offense Evals | | | ◆ | | | | | | ◆ | | | | | | ◆ | | | | | | ◆ | | | | | | ◆ | | | | | | ◆ | | | |
| Field Exercises | | | | | | | | | | | | | | | | | ◆ | | | | | | | | | | | | | | | | | ◆ | | |

- Schedule emphasizes early and frequent experimentation
- Field exercises with transition partners (PACOM, PACFLT, AFRL, DISA) drive transition
- TA1-4 performers' test plans define scenarios and metric measurement, under scrutiny of TA5
- Applications and protocols of potential interest for experiments: Global Command and Control System (GCCS), Web, Session Initiation Protocol (SIP), IRC, MapReduce and other cloud programming models, File Transfer Protocol (FTP)

# Important Points From BAA

- Areas out of scope for XD3:
  - Malware detection, or compromise of hosts running XD3 systems
  - Detection of DDoS traffic within network, or traceback techniques, unless techniques directly and uniquely support TA1-TA3 program goals
  - Wireless anti-jam technologies
  - Techniques that are applicable only to the protection of static content
- Proposals must clearly state the context for the proposed technical approach - what kind of networks, applications, and scale are to be addressed?
- Proposals must define metrics relevant to their approaches and contexts, and describe the envisioned testing environment and procedures
  - Should clearly support the main elements of the technical approach
- Individual TAs have additional specific requirements – see BAA
- Heed the BAA evaluation criteria including (but not limited to):
  - Is the approach feasible and achievable?
  - Have you identified technical risks (some aspect of your approach that may not work) and mitigation plans?
  - Does the approach produce a revolutionary, high-payoff result?
  - Are the costs realistic?

# Break

- The XD3 Program Q&A session will begin at 1600.

# Extreme DDoS Defense (XD3)

Stuart Wagner
Program Manager
Information Innovation Office (I2O)
DARPA

September 2, 2015

# Audience Q&A

- XD3 Program Q&A Session


www.darpa.mil